Order Code RS21283
Updated January 31, 2003

CRS Report for Congress
Received through the CRS Web

Homeland Security: Intelligence Support

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Summary

Legislation establishing a Department of Homeland Security (DHS) (P.L. 107-296) includes provisions for an information analysis element within the new department. It does not transfer to DHS existing government intelligence and law enforcement agencies, but envisions an analytical office utilizing the products of other agencies–both unevaluated information and finished reports–to provide warning of terrorist attacks, assessments of vulnerability, and recommendations for remedial actions at the federal, state, and local levels and by the private sector. This report examines the information analysis function and the sharing of information among federal agencies but does not address provisions in the proposed legislation governing the sharing of intelligence with state and local officials; it notes a recent Administration proposal to establish a new Terrorist Threat Integration Center; it will be updated as circumstances warrant.

Introduction

Better intelligence is held by many observers to be a crucial factor in preventing future terrorist attacks. Concerns have been expressed that no single agency or office in the federal government prior to September 11, 2001 was in a position to "connect the dots" between diffuse pieces of information that might have provided clues to the planned attacks. Testimony before the two intelligence committees' Joint Inquiry on the September 11 attacks indicated that significant information in the possession of intelligence and law enforcement agencies was not fully shared with other agencies and that intelligence on potential terrorist threats against the United States was not fully exploited.

For many years, the sharing of intelligence and law enforcement information was effected by administrative policies and statutory prohibitions. Beginning in the early 1990s, however, much effort has gone into improving interagency coordination.[1] In addition, a number of statutory obstacles have been removed by the USA-Patriot Act of

[1] For background on this issue, see CRS Report RL30252, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, by Richard A. Best, Jr.

2001 and other legislation.[2] Nevertheless, there has been no one place where the analytical effort is centered; the Department of Homeland Security (DHS) is designed to remedy that perceived deficiency.

Background

The Bush Administration's legislative proposal for a Department of Homeland Security, released July 16, 2002, was incorporated in H.R. 5005, introduced on June 24, 2002 by Representative Armey. Title II of the bill, Information Analysis and Infrastructure Protection, as subsequently amended and passed by the House on July 26, included provisions to establish an Intelligence Analysis Center to give intelligence support to the homeland security effort and to identify priorities for measures to protect key sources and critical infrastructures. In the Senate, Senator Lieberman had introduced legislation (S. 2452) to establish a Department of National Homeland Security on May 2, 2002. The original version of S. 2452 did not address the intelligence function, but subsequent amendments in the nature of a substitute included provisions establishing a Directorate of Intelligence as an integral part of the new department. After the November 2002 elections a modified version of homeland security legislation was introduced by Representative Armey and passed by the House on November 13, 2002. Subsequently, both House and Senate passed an amended version of H.R. 5005, and the bill was signed by the President on November 25, 2002, becoming P.L. 107-296.

The final version would establish a Directorate for Information Analysis and Infrastructure Protection headed by an Under Secretary for Information Analysis and Infrastructure Protection (appointed by the President by and with the advice and consent of the Senate) with an Assistant Secretary of Information Analysis (appointed by the President). The legislation, especially the Information Analysis section, seeks to promote close ties between intelligence analysts and those responsible for assessing vulnerabilities of key U.S. infrastructure. The bill envisions an intelligence entity focused on receiving and analyzing information[3] from other government agencies and using it to provide warning of terrorist attacks and for addressing vulnerabilities that terrorists could exploit.

DHS is not intended to duplicate the collection effort of intelligence agencies; it will not have its own agents, satellites, or signals intercept sites. Major intelligence agencies are not transferred to the DHS, although some DHS elements, including Customs and the Coast Guard, will continue to collect information that is crucial to analyzing terrorist threats.

The information analysis element within DHS will have the responsibility for acquiring and reviewing information from the agencies of the Intelligence Community, from law enforcement agencies, state and local government agencies, and unclassified publicly available information (known as open source information or "osint") from books,

---

[2] See CRS Report RL31377, *The USA Patriot Act: A Legal Analysis*, by Charles Doyle; and CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework*, by Elizabeth Bazan.

[3] Some writers distinguish between information and intelligence; the former being unanalyzed information the latter being the result of analysis. In practice, however, the terms are often used interchangeably and the distinction will not be observed in this report.

periodicals, pamphlets, the Internet, media, etc. The legislation is explicit that, "Except as otherwise directed by the President, the Secretary [of DHS] shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructures or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government."[4]

DHS analysts would be charged with using this information to identify and assess the nature and scope of terrorist threats; produce comprehensive vulnerability assessments of key resources and infrastructure, to identify priorities for protective and support measures by DHS, by other agencies of the federal government, state and local government agencies and authorities, the private sector, and other entities. They will disseminate information to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the U.S. The intelligence element is also charged with recommending measures necessary for protecting key resources and critical infrastructure in coordination with other federal agencies.

DHS would be responsible for ensuring that any material received is protected from unauthorized disclosure and handled and used only for the performance of official duties. (This provision addresses a concern that sensitive personal information made available to DHS analysts could be misused.) Intelligence information would be transmitted, retained, and disseminated consistent with policies established under the authority of the Director of Central Intelligence (DCI) to protect intelligence sources and methods and similar authorities of the Attorney General concerning sensitive law enforcement information.[5]

---

[4] Section 202(a)(1). The language provides for a presidential exception that might arise because of particularly sensitive information; some observers also argue that under any circumstances the President has a constitutional authority to control the dissemination of intelligence information.

[5] The DCI's authority for protecting intelligence sources and methods is set forth in 50 USC 403-3(c)(6).The Attorney General's authorities for safeguarding law enforcement information are diffuse; see, *e.g.*, 18 USC 2511 (interception and disclosure of wire, oral, or electronic communications prohibited, exceptions); 18 USC 2517 (authorization for disclosure and use of intercepted wire, oral, or electronic communications); 21 USC 190(e) (public disclosure of significant foreign narcotics traffickers and required reports, exclusions of certain information).

Issues Under Discussion

DHS Role in the Intelligence Community. The U.S. Intelligence Community, consists of the Central Intelligence Agency (CIA) and some 14 other agencies;[6] it provides information in various forms to the White House and other federal agencies (as well as to Congress). In addition, law enforcement agencies, such as the Federal Bureau of Investigation (FBI), also collect information for use in the federal government[7].

Within the Intelligence Community, priorities for collection (and to some extent for analysis) are established by the DCI,[8] based in practice on inter-agency discussions. Being "at the table" when priorities are discussed, it is widely believed, helps ensure equitable allocations of limited collection resources. The legislation would make the DHS element concerned with analyses of foreign intelligence information a member of the Intelligence Community, thus giving DHS a formal role when intelligence collection and analysis priorities are being addressed. It will also facilitate access to intelligence databases and other analytical resources. Some observers have expressed concern that this provision will involve DHS in extensive Intelligence Community staff responsibilities and would require more personnel resources than currently envisioned for DHS, thereby detracting from the intended focus on analysis of terrorist threats.

A similar situation has long existed in the State Department which has a Bureau of Intelligence and Research (INR) that is also a component of the Intelligence Community. Charged with providing intelligence input to the policymaking process, INR has had to strive to avoid letting policy goals of the Department influence its intelligence judgments. Most observers credit INR with having performed responsibly over the years. Being a component of the Intelligence Community has allowed INR to have direct and close access to intelligence data and analysis as well as to influence the establishment of collection and analysis priorities.

The Question of "Raw" Intelligence. There has been some discussion in the media whether DHS will have access to "raw" intelligence or only to finished analytical products, but these reports may reflect uncertainty regarding the definition of "raw" intelligence. A satellite photograph standing by itself might be considered "raw" data, but it would be useless unless something were known about where and when it was taken. Thus, satellite imagery supplied to DHS would under almost any circumstances have to have some analysis included. The same would apply to any signals intercepts. Reports from human agents present special challenges. Some assessment of the reliability of the source would have to be provided to DHS, but information that would identify a specific individual would normally be retained within a very small number of intelligence officials; the further such sensitive information is spread, the greater the danger of unauthorized disclosure and harm to the source. Observers believe that in almost all cases analysts can work without knowing the name of a specific source.

---

[6] Defined by 50 USC 401a(4). (Membership in the Intelligence Community has changed over the years; in 2001 the Coast Guard acquired the status of a member of the Intelligence Community pursuant to section 105 of P.L. 107-108, the FY2002 Intelligence Authorization Act.)

[7] 28 USC 533 provides information collecting authority to the Justice Department and the FBI.

[8] 50 USC 403-3(c)(2).

The issue of the extent and nature of information forwarded to DHS may become crucial to the effectiveness of the new department. Reviewing copies of summary reports prepared by existing agencies is seen by some observers as inadequate for the task of putting together a meaningful picture of terrorist capabilities and intentions and providing timely warning. On the other hand, there is a need to ensure that DHS analysts are not inundated with vast quantities of data and that highly sensitive information is not given wider dissemination than absolutely necessary.[9] Structuring the appropriate data flow and addressing the tendency of existing agencies to resist wider dissemination of information is expected to be a daunting challenge as DHS begins to function.

Open Source Information (Osint). Information from unclassified sources–books, pamphlets, periodicals, Internet sources, television and radio programs–is arguably an important resource for gaining information about terrorist groups and the larger political movements with which they are associated. There are different views regarding the emphasis to which intelligence agencies should give to open source information. DCI George Tenet in prepared testimony for the Senate Government Affairs Committee on June 27, 2002, stated that "In every possible case, we will provide intelligence at the lowest permissible level of classification, including sensitive, but unclassified."[10] Pointedly, he did not include open source information. DHS may have to undertake procedures to collect and analyze osint without support from intelligence agencies.

Analytical Quality. The key test for the DHS will be the quality of the analytical product–whether terrorist groups can be identified and warning given of plans for attacks on the U.S. While most observers acknowledge that focusing in one office the responsibility for identifying terrorist threats will remedy a fundamental limitation of existing arrangements, it is also understood that creating such an office will be difficult. The types of information that have to be analyzed come from disparate sources and require a variety of analytical skills that are not in plentiful supply. Academic institutions prepare significant numbers of linguists and area specialists, but training in the inner workings of clandestine terrorist entities is less often undertaken. Analysts with law enforcement backgrounds may not be attuned to the foreign environments from which terrorist groups emerge. DHS will begin with analysts detailed from existing intelligence and law enforcement agencies along with, presumably, some newly hired personnel. It will be necessary that previous bureaucratic competitors merge into an effective office and that a culture of objectivity and adherence to high standards be established from the outset.

The Terrorist Threat Integration Center. President Bush in his 2003 State of the Union address called for the establishment of a new Terrorist Threat Integration Center that would merge and analyze all threat information in a single location. The

---

[9] See Dan Eggen and John Mintz, "Homeland Security Won't Have Diet of Raw Intelligence; Rules Being Drafted to Preclude Interagency Conflict," *Washington Post*, December 6, 2002, p. A43.

[10] Testimony of Hon. George J. Tenet, U.S. Congress, Senate, 107th Congress, 2d session, Committee on Governmental Affairs, *A Review of the Relationship Between a Department of Homeland Security and the Intelligence Community*, Hearings, June 26 and 27, 2002, S. Hrg. 107-562, p. 69.

center is to be headed by a senior government official who would be appointed by the DCI in consultation with the FBI Director, the Attorney General, the Secretary of Defense, and the Secretary of DHS; the official will report to the DCI. Although details regarding the new center have not yet been made public, its major responsibilities are to "integrate terrorist-related information collected domestically and abroad" and to provide "terrorist threat assessments for our national leadership."[11] Its proponents assert that it is needed to coordinate highly sensitive intelligence material. Some observers suggest that these functions appear to duplicate responsibilities of the Information Analysis and Infrastructure Protection Division of DHS. By establishing a new center within the Intelligence Community, it is suggested, the DCI might seek to avoid releasing sensitive unevaluated information to a new and untested agency (DHS) that is mostly outside the Intelligence Community. Other observers express concern that the DCI's role in the new Threat Integration Center, responsible for the analysis of domestically collected information and for maintaining "an up-to-date database of known and suspected terrorists that will be accessible to federal and non-federal officials and entities,"[12] might run counter to the statutory provision that excludes the CIA from "law enforcement or internal security functions."[13]

Conclusion

Legislation creating a homeland security department recognizes the crucial importance of intelligence to the counterterrorist effort. It proposes an analytical office within DHS that will be able to draw upon the information gathering resources of other government agencies and of the private sector. It envisions the DHS information analysis entity working closely with other DHS offices, other federal agencies, state and local officials, and the private sector to devise strategies and programs to protect U.S. vulnerabilities and to provide warning of specific attacks. It provides for maintaining the security of classified and sensitive information and require its use only for official purposes. The success of a DHS intelligence entity will, however, be largely dependent upon the quality of leadership, the skills of analysts, and the cooperation provided by federal, state, local, and private agencies.

---

[11] White House Fact Sheet, "Strengthening Intelligence to Better Protect America," January 28, 2003.

[12] Ibid.

[13] 50 USC 403-3(d)(1).